A Physical Layer Network Coding Based Modify-and-Forward with Opportunistic Secure Cooperative Transmission Protocol

Quoc-Tuan Vien, Tuan Anh Le, Huan X. Nguyen, and Tho Le-Ngoc

***Abstract*—This paper investigates a new secure relaying scheme, namely physical layer network coding based modify-and-forward (PMF), in which a relay node linearly combines the decoded data sent by a source node with an encrypted key before conveying the mixed data to a destination node. We first derive the general expression for the generalized secrecy outage probability (GSOP) of the PMF scheme and then use it to analyse the GSOP performance of various relaying and direct transmission strategies. The GSOP performance comparison indicates that these transmission strategies offer different advantages depending on the channel conditions and target secrecy rates, and relaying is not always desirable in terms of secrecy. Subsequently, we develop an opportunistic secure transmission protocol for cooperative wireless relay networks and formulate an optimisation problem to determine secrecy rate thresholds (SRTs) to dynamically select the optimal transmission strategy for achieving the lowest GSOP. The conditions for the existence of the SRTs are derived for various channel scenarios.**

***Index Terms*—Wireless relay networks; physical layer network coding; decode-and-forward; modify-and-forward; cooperative jamming.**

I. Introduction

Physical-layer security has recently attracted the interest of broader communications societies [1], especially in cooperative wireless relay networks (CWRNs) [2]–[6] where user cooperation has been identified as an innovative change enabling multi-hop communications [7]–[9]. The connection between a subscriber and a legitimate transmitter can be realised with the assistance of a relay node employing either amplify-and-forward (AF) or decode-and-forward (DF) protocols [10]. Over the wireless media, the eavesdropper and/or attacker can overhear the message from both the transmitter and the relay nodes. Therefore, in order to protect data from vulnerable attacks in the CWRNs, the security of both the direct and relaying links needs to be investigated.

From the physical-layer perspective, information-theoretic approach has been shown to be able to provide secure communications between legitimate users by using jamming signals and appropriate channel coding [2]. A basic approach was originally proposed in [11] for a noiseless cipher system where the data is encrypted by simply XORing with a shared secret key. The noisy channel was then investigated in [12] where Wyner first introduced the concept of wiretap channel. It is shown that the innate irregularity and diversity of the message can confuse the eavesdropper, and thus strengthen the legitimate communications. Specifically, independent transmitters can help in transmitting jamming signals to enhance the secrecy rate of the legitimate users [13]–[15]. However, such cooperative jamming (CJ) can cause interferences that reduce the decoding rate at the legitimate receivers [16]–[18]. Another approach of the CJ is noise forwarding [19] where a relay node sends extra irregularity to direct as haphazardly chosen codewords from codebook known to both the legitimate sender and the beneficiary [20].

Motivated by the concept of network coding (NC) for improving the throughput of lossless networks [21], [22], a vast number of works have investigated the application of physical-layer NC (PNC) in CWRNs, e.g. in [23]–[29], and secure NC has also been proposed in [30], [31] to improve the security of wiretap channels. The principle of the PNC is that the relays perform algebraic linear/logic operations on received packets from multiple transmission source nodes and then forward the combined packets to the destination nodes in the subsequent transmissions.

Focusing on secure communications in CWRNs, various relaying strategies were investigated in [32]–[34]. Specifically, secure AF and DF schemes were analysed in [32], [33]. Modify-and-forward (MF) cooperation scheme was proposed in [34] where the relay first modifies the message received from the source in the first time slot and then forwards the modified message to the destination in the second time slot. In the MF scheme, the modification process at the relay is assumed to be inherently shared between legitimate users, and thus only the interested destination can recover the original message. This MF approach yields an enhanced secrecy performance in comparison with other relaying techniques. However, the work in [34] assumed that the eavesdropper can only decode the message from the source in the first time slot, which limits its application in practice since the eavesdropper could also overhear and decode a part of the message from the relay in the second time slot. Additionally, over the wireless media, the channel dedicated for sharing knowledge between the relay and the destination suffers from fading and background noise, which may cause a considerable performance degradation. Furthermore, it can be noticed that the relaying schemes do not always provide the best performance as they depend on the channel quality of various links and target secrecy rate. Therefore, it is crucial to address these practical

Q.-T. Vien, T. A. Le, and H. X. Nguyen are with the School of Science and Technology, Middlesex University, United Kingdom. Email: {q.vien; t.le; h.nguyen}@mdx.ac.uk.

T. Le-Ngoc is with the Department of Electrical and Computer Engineering, McGill University, Montreal, Canada. Email: tho.le-ngoc@mcgill.ca.

issues as well as providing a numerical approach in finding the optimal scheme among the direct and relaying schemes with respect to the channel environment and the QoS requirement of secrecy rate.

In this paper, inspired by the principle of PNC, we first propose a new secure relaying scheme, namely secure PNC-based MF (PMF), to cope with the practical security issue of the imperfectly shared knowledge of the message modification between relay and destination in the conventional MF scheme, i.e. [34]. Furthermore, the proposed scheme takes into account a practical scenario that the eavesdropper can overhear and attempt to decode the message from both the source and the relay in CWRNs. By deriving the generalized secrecy outage probability (GSOP) of the PMF scheme with respect to other direct and relaying schemes,[1] the usage of the relay is shown not to be always beneficial, especially when the link between the source and the relay and (or) the link between the relay and the destination suffer(s) from severe fading and noise. This fact, however, is brought into question when the relay should be exploited to provide a higher secure communication, and thus motivates us to propose an opportunistic secure transmission protocol for the CWRNs. The main contributions of this paper can be summarised as follows:

- *A novel PMF scheme for legitimate users*: In the proposed PMF scheme, the PNC operation at the relay can restrict the eavesdropper to receiving only part of information from the relay rather than overhearing the full message. This PNC operation also differentiates the proposed scheme from the cryptographic techniques with only encrypted key. Furthermore, the assumption of perfectly shared information of PNC coefficients and encrypted key[2] between the relay and destination is relaxed, while only channel statistics are assumed to be known at the destination.
- *Derivation of GSOP*: GSOP is considered to link the concept of physical layer security and eavesdropper decodability [38], [39]. The derived GSOP for the proposed PMF scheme reveals not only its effectiveness in relation to the conventional direct transmission (DT) [40] and other relaying transmission (RT) schemes, such as DF [32], CJ [13] and MF [34], but also the level of secrecy requirements from the cryptographic perspective. In particular, this derived GSOP is shown to be a general expression also for the DF and MF schemes. It indicates that the DF scheme is a special case of the PMF scheme when neither encryption nor PNC operation is performed at the relay and the MF scheme can be regarded as an ideal case of the PMF scheme with no PNC operation and when the link between the relay and eavesdropper is neglected.
- *GSOP comparison of different schemes*: The proposed PMF scheme is shown to provide an enhanced security with a lower GSOP under certain channel link quality, channel knowledge and target secrecy rate when compared to DT, DF and CJ schemes. Moreover, the GSOP of the PMF scheme approaches that of the MF scheme which is regarded as a lower bound of the PMF scheme in an ideal scenario. It is further noticed that the DT scheme without the assistance of the relay can achieve a higher secrecy performance over all RT schemes at a high target secrecy rate, especially when the direct link is of very high quality. These remarkable facts accordingly mean that none of these schemes are able to ensure the highest secrecy at all times given variant channel conditions and secrecy rate requirements.
- *A new opportunistic secure transmission protocol for CWRNs*: The proposed protocol aims at finding an optimal protocol among DT and RT schemes that achieves the best secrecy performance with the lowest GSOP. It is shown that there exist secrecy rate thresholds (SRTs) which are the crossing points between the GSOPs of various schemes. The optimisation problem is thus turned into finding the SRTs with respect to channel conditions and secrecy rate requirements. Furthermore, the conditions of the channel quality are derived for the existence of the SRTs. The derived SRTs are shown to not only facilitate the finding of the optimal scheme for a secure CWRN, but also help in determining if the relay could be relied on in the practical CWRNs.

The rest of this paper is organised as follows: Section II describes the system model of a typical CWRN in the presence of an eavesdropper. Section III presents the proposed PMF scheme. The GSOP analysis of the PMF scheme is presented in Section IV in comparison with DT, DF, CJ and MF schemes. The opportunistic secure transmission protocol for the CWRN is developed in Section V where the SRTs are determined. Numerical and simulation results are presented in Section VI to validate the concepts. Finally, Section VII draws the main conclusions from this paper.

II. System Model

Figure 1 illustrates the system model of a CWRN under investigation consisting of a source node $\mathcal{S}$, a destination node $\mathcal{D}$ and a relay node $\mathcal{R}$ in the presence of an eavesdropper node $\mathcal{E}$. It is assumed that there exists a direct link $\mathcal{S} \rightarrow \mathcal{D}$ and thus $\mathcal{S}$ may transmit a data packet to $\mathcal{D}$ either with or without the assistance of $\mathcal{R}$. In Fig. 1, $\mathcal{E}$ is assumed to be located between $\mathcal{S}$ and $\mathcal{D}$ and in the vicinity of $\mathcal{R}$. Therefore, there exist two wiretap links from both $\mathcal{S}$ and $\mathcal{R}$ to $\mathcal{E}$.

The communication channel between nodes $\mathcal{A}$ and $\mathcal{B}$, $\mathcal{A}, \mathcal{B} \in \{\mathcal{S}, \mathcal{R}, \mathcal{E}, \mathcal{D}\}$, $\mathcal{A} \neq \mathcal{B}$, is assumed to experience identical and independently distributed quasi-static Rayleigh flat fading where all channel gains are time-invariant over the whole transmission of a data packet and vary independently in the next data packet. The instantaneous and average signal-to-noise ratio (SNR) or signal-to-interference-plus-noise ratio

[1]This work is extended from [35], [36] where only results of the classical SOP were provided for the PMF scheme in the scenario that the eavesdropper can overhear the message in the first time slot, but does not attempt to decode the message from the relay due to its lack of knowledge of the modification process at the relay. We now take a further step by providing a detailed analysis for deriving the GSOP of the PMF scheme to link the concept of physical layer security and cryptography. Also, this work considers the general scenario when the eavesdropper can overhear and attempts to decode the message from both the source and the relay.

[2]The encrypted key in the proposed scheme is generated at the physical layer as a training sequence. The design of a physical layer encryption scheme can be referred to in [37].

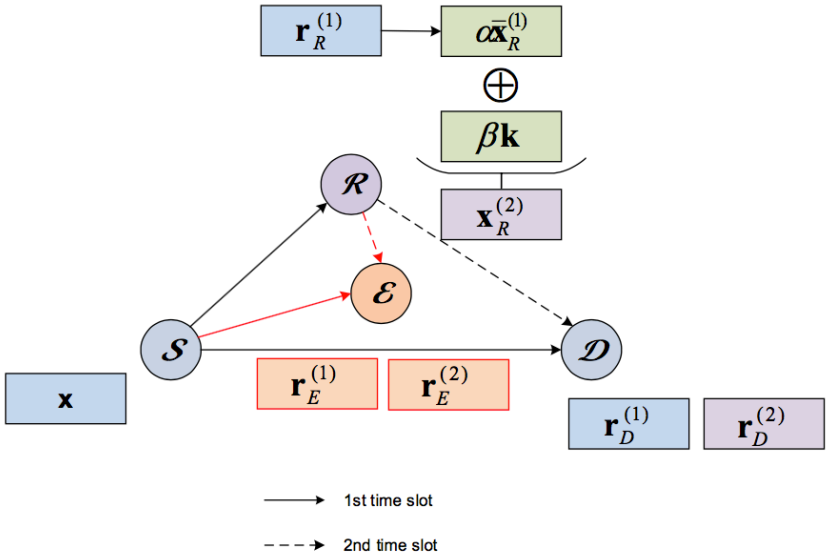

Fig. 1: System model of a CWRN in the presence of an eavesdropper.

(SINR) of the link $\mathcal{A} \to \mathcal{B}$ are denoted by $\gamma_{\mathcal{AB}}$ and $\bar{\gamma}_{\mathcal{AB}}$, respectively. The probability density function (pdf) and cumulative distribution function (cdf) of a random variable X are denoted by $f_X(\cdot)$ and $F_X(\cdot)$, respectively.

In the DT scheme, $\mathcal{S}$ transmits data directly to $\mathcal{D}$, while in the RT scheme, the cooperative data transmission from $\mathcal{S}$ to $\mathcal{D}$ is realised via two time slots as follows:

i) *Time slot 1*: $\mathcal{S}$ transmits the data packet to both $\mathcal{R}$ and $\mathcal{D}$;
ii) *Time slot 2*: $\mathcal{R}$ processes the data packet received from $\mathcal{S}$ prior to forwarding the processed data to $\mathcal{D}$.

III. Proposed PMF Scheme

In this section, we introduce the data transmission, decoding and encryption process in our proposed PMF scheme for enhancing the security of a CWRN as shown in Fig. 1.

In the first time slot, $\mathcal{S}$ transmits a data packet $\mathbf{x}$ to both $\mathcal{R}$ and $\mathcal{D}$. Over the eavesdropping channel, $\mathcal{E}$ also receives the data packet from $\mathcal{S}$. The received signal at node $\mathcal{X}$, $\mathcal{X} \in \{\mathcal{R}, \mathcal{D}, \mathcal{E}\}$, is given by

$$\mathbf{r}_{\mathcal{X}}^{(1)} = \sqrt{\Lambda_{\mathcal{S}}} h_{\mathcal{SX}} \mathbf{x} + \mathbf{n}_{\mathcal{X}}^{(1)}, \tag{1}$$

where $\Lambda_{\mathcal{S}}$ is the power of the source $\mathcal{S}$, $h_{\mathcal{SX}}$ is the channel gain between $\mathcal{S}$ and $\mathcal{X}$, and $\mathbf{n}_{\mathcal{X}}^{(1)}$ is an independent circularly symmetric complex Gaussian (CSCG) noise vector at node $\mathcal{X}$ with each entry having zero mean and variance of σ_0^2. Then, $\mathcal{X}$ decodes the data from $\mathcal{S}$, which is denoted by $\bar{\mathbf{x}}_{\mathcal{X}}^{(1)}$.

In the second time slot, after decoding the data packet received from $\mathcal{S}$,[3] the relay node $\mathcal{R}$ randomly and linearly combines the decoded data, i.e. $\bar{\mathbf{x}}_{\mathcal{R}}^{(1)}$, with the encrypted key (denoted by $\mathbf{k}$) using randomised PNC approach as follows:

$$\mathbf{x}_{\mathcal{R}}^{(2)} = \alpha \bar{\mathbf{x}}_{\mathcal{R}}^{(1)} + \beta \mathbf{k}, \tag{2}$$

where α and β are random PNC coefficients satisfying $\alpha^2 + \beta^2 = 1$ and $\alpha \neq 0$.

Through the second hop, $\mathcal{D}$ is expected to receive the data from $\mathcal{R}$, while $\mathcal{E}$ could overhear the same information. The received signal at node $\mathcal{Y}$, $\mathcal{Y} \in \{\mathcal{D}, \mathcal{E}\}$, is given by

$$\mathbf{r}_{\mathcal{Y}}^{(2)} = \sqrt{\Lambda_R} h_{\mathcal{RY}} \mathbf{x}_{\mathcal{R}}^{(2)} + \mathbf{n}_{\mathcal{Y}}^{(2)}, \tag{3}$$

where $\Lambda_{\mathcal{R}}$ is the power of the relay $\mathcal{R}$, $h_{\mathcal{RY}}$ is the channel gain between $\mathcal{R}$ and $\mathcal{Y}$, and $\mathbf{n}_{\mathcal{Y}}^{(2)}$ is a CSCG noise vector at node $\mathcal{Y}$ with each entry having zero mean and variance of σ_0^2. Substituting (2) into (3), we obtain

$$\mathbf{r}_{\mathcal{Y}}^{(2)} = \sqrt{\Lambda_{\mathcal{R}}} h_{\mathcal{RY}} \alpha \bar{\mathbf{x}}_{\mathcal{R}}^{(1)} + \sqrt{\Lambda_{\mathcal{R}}} h_{\mathcal{RY}} \beta \mathbf{k} + \mathbf{n}_{\mathcal{Y}}^{(2)}. \tag{4}$$

Although the PNC coefficients and encrypted key are only shared between the legitimate users, $\mathcal{E}$ can still decode the data sent from $\mathcal{R}$ by treating these unknowns as interference and performing maximum ratio combining (MRC) of the signals received in both time slots from $\mathcal{S}$ and $\mathcal{R}$. On the other hand, it is likely that $\mathcal{D}$ can decode the interested data given the shared information between $\mathcal{S}$, $\mathcal{R}$ and $\mathcal{D}$. However, at $\mathcal{D}$, imperfectly shared knowledge of the PNC coefficients and encrypted key can also take place due to the inherent fading and noises of the wireless channels. In other words, we need to consider the following two cases:

i) *PMF-perfect*: With perfectly shared knowledge of α, β and $\mathbf{k}$, $\mathcal{D}$ is able to decode the data from $\mathcal{R}$ in the second time slot by eliminating α, β and $\mathbf{k}$ in (4).
ii) *PMF-imperfect*: This case implies that $\mathcal{D}$ may only obtain partial knowledge of α, β and $\mathbf{k}$ (either of them but not all). $\mathcal{D}$ can employ maximum likelihood detection to

[3]Note that a trusted relay channel is considered in this work where the relay can decode the confidential message prior to processing and forwarding it to the destination. The scenario of untrusted relay channels can be coped with by applying modulo-and-forward scheme at the relay with nested lattice encoding at the source as in [41].

recover the data in the second time slot given the known channel statistics of the link $\mathcal{R} \to \mathcal{D}$.

Remark 1 (*Improved Security With the Proposed PMF*)**.** As shown in (4), in order to encrypt the data packet forwarded from the relay node $\mathcal{R}$, two layers of security are integrated into the PMF scheme including the PNC coefficients, i.e. α and β, and the encrypted key, i.e. $\mathbf{k}$. Such modification process at $\mathcal{R}$ can thus confuse the eavesdropper $\mathcal{E}$ from overhearing the full message from $\mathcal{R}$, which accordingly results in a more secure relay communications between legitimate users. It can also be noticed that the cryptographic techniques correspond to the scenario when the PNC is not employed at $\mathcal{R}$, and thus only the encrypted key is required at the eavesdropper to decode the overheard packet.

Remark 2 (*DF & MF - Special Cases of the Proposed PMF*)**.** It can be seen in (4) that the conventional DF scheme can be deduced from the PMF scheme by setting $\alpha = 1$ and $\beta = 0$, which means there is no encrypted key and no PNC operation at $\mathcal{R}$. In relation to the work in [34], the MF scheme assumes that $\mathcal{E}$ omits the message from $\mathcal{R}$ due to the unavailability of the modification process performed at $\mathcal{R}$, and thus can be regarded as a special case of the PMF when the link $\mathcal{R} \to \mathcal{E}$ does not exist. However, it is worth mentioning that such assumption of no decoding process performed at $\mathcal{E}$ in the second time slot may restrict the application of the MF scheme in practice. Instead, our work considers a general scenario dealing with the issue when $\mathcal{E}$ can partially decodes the message from $\mathcal{R}$ by treating the encrypted key as interference.

Regarding the complexity of the proposed PMF scheme at the relay, only arithmetic functions are required to combine the data packet and the encrypted key. From (2), it can be seen that there are a total of M additions and $2M$ multiplications where M is the data packet length. In other words, as compared to the conventional DF scheme (which simply decodes and amplifies the data packet received from the source), the security of the proposed scheme comes at the cost of an increase in computational complexity. Modulo addition (instead of linear addition) can be used with lattice code (as in [41]) in the scenario of untrusted relay channels for energy savings.

IV. Generalized Secrecy Outage Probability Analysis

In this section, we first derive the GSOP of the proposed PMF scheme for a CWRN considering the general scenario of imperfectly shared information of message modification between relay and destination, i.e. PMF-imperfect scheme. For comparison, the GSOP of DT scheme [40] and other RT schemes, including DF [32], CJ [13] and MF [34], are also provided to verify the effectiveness of the PMF scheme as well as motivating us to propose an opportunistic secure transmission protocol which will be presented in the following section.

The GSOP is defined as the probability that the wireless system fails to achieve a target secrecy rate subject to secrecy requirements [38], i.e.

$$P_{out} \triangleq \Pr\left\{\frac{C_s}{R_s} < \theta\right\}, \tag{5}$$

where R_s is the target secrecy rate, C_s is the instantaneous secrecy capacity and θ, $0 < \theta \leq 1$, is the minimum acceptable value of the fractional equivocation, i.e. the ratio of C_s to R_s. Here, θ represents the level of secrecy requirements. A particular case is when $\theta = 1$, then the GSOP turns into the classical SOP. In (5), C_s can be computed by

$$C_s = \max\{C_d - C_e, 0\} = [C_d - C_e]^+, \tag{6}$$

where C_d is the instantaneous channel capacity of the legitimate links, C_e is the instantaneous channel capacity of the eavesdropper links, and $[x]^+ \triangleq \max\{x, 0\}$. Intuitively, it can be observed in (6) that, to have a secure communication with a positive secrecy capacity, the legitimate links must be dominant over the eavesdropper links.

A. PMF Scheme

We now proceed to derive C_d and C_e of the PMF scheme. Taking into account both direct and relaying links with decoding and PNC operation at $\mathcal{R}$, the maximum rate for reliable data communications between $\mathcal{S}$ and $\mathcal{D}$ can be expressed by

$$C_d = \min\left\{\frac{1}{2}\log_2(1+\gamma_{\mathcal{SR}}), \frac{1}{2}\log_2(1+\gamma_{\mathcal{SD}}+\gamma_{\mathcal{RD}})\right\}, \tag{7}$$

where $\gamma_{\mathcal{SR}}$ and $\gamma_{\mathcal{SD}}$ denote the instantaneous SNR of the link $\mathcal{S} \to \mathcal{R}$ and $\mathcal{S} \to \mathcal{D}$, respectively, in the first time slot, and $\gamma_{\mathcal{RD}}$ denotes the instantaneous SINR of the link $\mathcal{R} \to \mathcal{D}$ in the second time slot. Here, the instantaneous SNR $\gamma_{\mathcal{SR}}$ and $\gamma_{\mathcal{SD}}$ can be respectively computed from (1) as

$$\gamma_{\mathcal{SR}} = \frac{\Lambda_{\mathcal{S}}|h_{\mathcal{SR}}|^2}{\sigma_0^2}, \tag{8}$$

$$\gamma_{\mathcal{SD}} = \frac{\Lambda_{\mathcal{S}}|h_{\mathcal{SD}}|^2}{\sigma_0^2}. \tag{9}$$

In the second time slot, $\mathcal{D}$ receives the combined data from $\mathcal{R}$ consisting of both the interested information and encrypted key. From (4), $\gamma_{\mathcal{RD}}$ can be determined by

$$\gamma_{\mathcal{RD}} = \frac{\Lambda_{\mathcal{R}}|h_{\mathcal{RD}}|^2\alpha^2}{\Lambda_{\mathcal{R}}|h_{\mathcal{RD}}|^2\beta^2 + \sigma_0^2}. \tag{10}$$

Due to the broadcast nature of the wireless channels, $\mathcal{E}$ can eavesdrop the data from $\mathcal{S}$ and $\mathcal{R}$ in both time slots. Such information leakage can be intuitively measured by comparing the uncertainty about the message before and after $\mathcal{E}$ receives it [42]. From an information theoretical point of view, this leakage is the mutual information and the maximum rate for reliable eavesdropping or the maximum leakage rate is the channel capacity of the eavesdropper link. Taking the advantage of both diversity branches with MRC approach, the maximum leakage rate at $\mathcal{E}$ is given by

$$C_e = \frac{1}{2}\log_2(1+\gamma_{\mathcal{SE}}+\gamma_{\mathcal{RE}}), \tag{11}$$

where $\gamma_{\mathcal{SE}}$ and $\gamma_{\mathcal{RE}}$ are respectively given by

$$\gamma_{\mathcal{SE}} = \frac{\Lambda_{\mathcal{S}}|h_{\mathcal{SE}}|^2}{\sigma_0^2}, \tag{12}$$

$$\gamma_{\mathcal{RE}} = \frac{\Lambda_{\mathcal{R}}|h_{\mathcal{RE}}|^2\alpha^2}{\Lambda_{\mathcal{R}}|h_{\mathcal{RE}}|^2\beta^2 + \sigma_0^2}. \quad (13)$$

Remark 3 (*Impact of PNC Coefficients on GSOP Performance*)**.** It can be seen in (10) and (13) that the PNC coefficients affect both the SINR of both legitimate link $\mathcal{R} \to \mathcal{D}$ and eavesdropping link $\mathcal{R} \to \mathcal{E}$ in the second time slot. In order to validate their impacts on the GSOP performance, for instance, let us consider a specific scenario when $\gamma_{\mathcal{SR}} > \gamma_{\mathcal{SD}} + \gamma_{\mathcal{RD}}$ and $\gamma_{\mathcal{SD}} \approx \gamma_{\mathcal{SE}}$. It can be shown that, as α increases (or β decreases), $(\gamma_{\mathcal{RD}} - \gamma_{\mathcal{RE}})$ increases if $|h_{\mathcal{RD}}|^2 \geq |h_{\mathcal{RE}}|^2$; otherwise, $(\gamma_{\mathcal{RD}} - \gamma_{\mathcal{RE}})$ decreases. This accordingly results in the change of the GSOP. The finding of the optimal PNC coefficients at $\mathcal{R}$ is worth to investigate taking into account all channel gains. In the general case, the knowledge of all these gains is required to be either perfectly known or estimated at $\mathcal{R}$. This is however beyond the scope of this work where $\mathcal{R}$ is only required to know the channel from $\mathcal{S}$ to decode the data packet prior to employing the random PNC.

Substituting (7) and (11) into (6), the secrecy capacity, i.e. C_S, can be obtained and the GSOP of the PMF can be thus derived from (5) as

$$P_{out}^{(PMF)} = \Pr\left\{\left[\log_2\left(\frac{1+\min\{\gamma_{\mathcal{SR}}, \gamma_{\mathcal{SD}}+\gamma_{\mathcal{RD}}\}}{1+\gamma_{\mathcal{SE}}+\gamma_{\mathcal{RE}}}\right)\right]^+ < 2\theta R_s\right\}. \quad (14)$$

In order to analyse (14), let us firstly find the pdf of $\gamma_{\mathcal{SR}}$, $\gamma_{\mathcal{SD}}$, $\gamma_{\mathcal{RD}}$, $\gamma_{\mathcal{SE}}$ and $\gamma_{\mathcal{RE}}$ defined in (8), (9), (10), (12) and (13), respectively. Since the links between nodes are assumed to experience Rayleigh flat fading, the pdf of the SNR $\gamma_{\mathcal{AB}}$, $\mathcal{AB} \in \{\mathcal{SR}, \mathcal{SD}, \mathcal{SE}\}$ is given by [43]

$$f_{\gamma_{\mathcal{AB}}}(\gamma_{\mathcal{AB}}) = \frac{1}{\bar{\gamma}_{\mathcal{AB}}} \exp\left(-\frac{\gamma_{\mathcal{AB}}}{\bar{\gamma}_{\mathcal{AB}}}\right), \quad (15)$$

while the pdf of the SINRs $\gamma_{\mathcal{RD}}$ and $\gamma_{\mathcal{RE}}$ can be obtained using the following Lemma 1.

Lemma 1. *If $X = c|Z|^2$, where c is a positive constant, Z is a zero-mean complex Gaussian random variable with variance of 1, and $Y = \frac{a^2 X}{b^2 X + 1}$, where $a^2 + b^2 = 1$ and $a \neq 0$, then the pdf of Y is given by*

$$f_Y(y) = \frac{a^2}{c(a^2 - b^2 y)^2} \exp\left[-\frac{y}{c(a^2 - b^2 y)}\right]. \quad (16)$$

Proof. See Appendix A. □

From the above Lemma 1, the pdf of the SINR $\gamma_{\mathcal{A'B'}}$, $\mathcal{A'B'} \in \{\mathcal{RD}, \mathcal{RE}\}$, can be expressed by

$$f_{\gamma_{\mathcal{A'B'}}}(\gamma_{\mathcal{A'B'}}) = \frac{\alpha^2}{\bar{\gamma}_{\mathcal{A'B'}}(\alpha^2 - \beta^2\gamma_{\mathcal{A'B'}})^2} \times \exp\left[\frac{-\gamma_{\mathcal{A'B'}}}{\bar{\gamma}_{\mathcal{A'B'}}(\alpha^2 - \beta^2\gamma_{\mathcal{A'B'}})}\right]. \quad (17)$$

Remark 4 (*General pdf of SINR $\gamma_{\mathcal{RD}}$ and $\gamma_{\mathcal{RE}}$*)**.** It can be observed that the pdf of the SNR in (15) is a special form of the pdf of the SINR in (17) when $\alpha = 1$ and $\beta = 0$. In the scenario that the encrypted key and PNC operation at $\mathcal{R}$ are known at $\mathcal{D}$, the proposed PMF is regarded as PMF-perfect scheme when $\gamma_{\mathcal{RD}}$ is given by (15). In case that such modification process at $\mathcal{R}$ is known at both $\mathcal{D}$ and $\mathcal{E}$, then both $\gamma_{\mathcal{RD}}$ and $\gamma_{\mathcal{RE}}$ are computed by (15). We then have a more special case of the PMF scheme which is indeed the conventional DF scheme as also noticed in Remark 2. However, it is worth noting that the eavesdropper in our work can overhear the message in both time slots but only a partial information can be recovered in the second time slot given imperfect knowledge of the modification process at $\mathcal{R}$. This accordingly reflects the novelty of our work in the GSOP analysis of the PMF scheme for CWRNs.

Given the pdf of all channel links in (15) and (17), further derivation of (14) leads to the following finding:

Theorem 1. *The GSOP of the proposed PMF scheme is obtained by* (18) *(see the top of next page), where*

$$I_1(x) \triangleq \int_0^x f_U(u) \int_{2^{-2\theta R_s}(1+x)-1-u}^{x-u} f_V(v)\, dv\, du, \quad (19)$$

$$I_2(x) \triangleq \int_0^x f_U(u) \int_0^{x-u} f_V(v)\, dv\, du, \quad (20)$$

$$f_X(x) = \frac{1}{\bar{\gamma}_{\mathcal{SR}}} \exp\left(-\frac{x}{\bar{\gamma}_{\mathcal{SR}}}\right), \quad (21)$$

$$f_Y(y) = \frac{1}{\bar{\gamma}_{\mathcal{SD}}} \exp\left(-\frac{y}{\bar{\gamma}_{\mathcal{SD}}}\right), \quad (22)$$

$$f_Z(z) = \frac{\alpha^2}{\bar{\gamma}_{\mathcal{RD}}(\alpha^2 - \beta^2 z)^2} \exp\left(-\frac{z}{\bar{\gamma}_{\mathcal{RD}}(\alpha^2 - \beta^2 z)}\right), \quad (23)$$

$$f_U(u) = \frac{1}{\bar{\gamma}_{\mathcal{SE}}} \exp\left(-\frac{u}{\bar{\gamma}_{\mathcal{SE}}}\right). \quad (24)$$

$$f_V(z) = \frac{\alpha^2}{\bar{\gamma}_{\mathcal{RE}}(\alpha^2 - \beta^2 v)^2} \exp\left(-\frac{v}{\bar{\gamma}_{\mathcal{RE}}(\alpha^2 - \beta^2 v)}\right), \quad (25)$$

Proof. See Appendix B. □

It is noted that the derivation of the closed-form expression for the GSOP of the proposed PMF in Theorem 1 is challenging. Nevertheless, the GSOP of the conventional DF and MF schemes in the following subsection can be derived from (18) as special cases of the PMF scheme.

B. DT Scheme

In DT scheme, the relay is assumed to be unavailable and thus, for fair comparison, $\mathcal{S}$ sends the encoded data to $\mathcal{D}$ using the power of $2\Lambda_{\mathcal{S}}$. The GSOP of the DT is given by [40]

$$P_{out}^{(DT)} = \Pr\left\{\left[\log_2\left(\frac{1+2\gamma_{\mathcal{SD}}}{1+2\gamma_{\mathcal{SE}}}\right)\right]^+ < \theta R_s\right\} = 1 - \frac{\bar{\gamma}_{\mathcal{SD}}}{\bar{\gamma}_{\mathcal{SD}} + 2^{\theta R_s}\bar{\gamma}_{\mathcal{SE}}} \exp\left(\frac{1-2^{\theta R_s}}{2\bar{\gamma}_{\mathcal{SD}}}\right). \quad (26)$$

$$
\begin{aligned}
P_{out}^{(PMF)} = &\int_{2^{2\theta R_s}-1}^{\infty} f_Y(y) \int_{y}^{\infty} f_X(x) \int_{x-y}^{\infty} f_Z(z) I_1(x)\, dz\, dx\, dy \\
&+ \int_{2^{2\theta R_s}-1}^{\infty} f_X(x) \int_{x}^{\infty} f_Y(y) I_1(x)\, dy\, dx \\
&+ \int_{0}^{2^{2\theta R_s}-1} f_Y(y) \int_{2^{2\theta R_s}-1}^{\infty} f_X(x) \int_{x-y}^{\infty} f_Z(z) I_1(x)\, dz\, dx\, dy \\
&+ \int_{0}^{2^{2\theta R_s}-1} f_Y(y) \int_{y}^{2^{2\theta R_s}-1} f_X(x) \int_{x-y}^{\infty} f_Z(z) I_2(x)\, dz\, dx\, dy \\
&+ \int_{2^{2\theta R_s}-1}^{\infty} f_X(x) \int_{2^{2\theta R_s}-1}^{x} f_Y(y) \int_{2^{2\theta R_s}-1-y}^{x-y} f_Z(z) I_1(y+z)\, dz\, dy\, dx
\end{aligned} \tag{18}
$$

C. CJ Scheme

Let us consider a typical CJ scheme in [13]. The principle of the CJ is that different transmitters transmit jamming signals with the aim of interfering the illegitimate receiver. In the context of the considered CWRN, $\mathcal{R}$ transmits jamming signals while $\mathcal{S}$ transmits the data to $\mathcal{D}$. Due to the autonomous property of the jamming signals, they may confuse $\mathcal{E}$ from eavesdropping the data; however, it can be noticed that such jamming signals could also harm $\mathcal{D}$. The GSOP of the CJ scheme can be computed by

$$
P_{out}^{(CJ)} = \Pr\left\{ \left[\log_2 \left(\frac{1+\dfrac{\gamma_{\mathcal{SD}}}{\gamma_{\mathcal{RD}}+1}}{1+\dfrac{\gamma_{\mathcal{SE}}}{\gamma_{\mathcal{RE}}+1}} \right) \right]^{+} < 2\theta R_s \right\}, \tag{27}
$$

where

$$
\gamma_{\mathcal{RD}} = \frac{\Lambda_{\mathcal{R}} |h_{\mathcal{RD}}|^2}{\sigma_0^2}. \tag{28}
$$

$$
\gamma_{\mathcal{RE}} = \frac{\Lambda_{\mathcal{R}} |h_{\mathcal{RE}}|^2}{\sigma_0^2}. \tag{29}
$$

Following [13], $P_{out}^{(CJ)}$ can be derived in closed form as

$$
\begin{aligned}
P_{out}^{(CJ)} = 1 - \frac{2^{-\delta}}{\bar{\gamma}_{\mathcal{RD}}\zeta} + \frac{2^{-\delta}}{\bar{\gamma}_{\mathcal{RD}}\bar{\gamma}_{\mathcal{RE}}\zeta^2} \Bigg[&\frac{2^{2\theta R_s}\bar{\gamma}_{\mathcal{SE}}(\zeta+1)}{\bar{\gamma}_{\mathcal{SD}}} \Xi\left(\frac{1+\vartheta}{\bar{\gamma}_{\mathcal{RE}}}\right) \\
&+ (\zeta-\vartheta)\Xi\left(\frac{1+\vartheta}{\vartheta}(\delta+\bar{\gamma}_{\mathcal{RD}}^{-1})\right)\Bigg],
\end{aligned} \tag{30}
$$

where $\delta \triangleq (2^{2\theta R_s}-1)\bar{\gamma}_{\mathcal{SD}}^{-1}$, $\vartheta \triangleq 2^{2\theta R_s}\bar{\gamma}_{\mathcal{SE}}\bar{\gamma}_{\mathcal{SD}}^{-1}$, $\zeta \triangleq \delta + \bar{\gamma}_{\mathcal{RD}}^{-1} - \vartheta\bar{\gamma}_{\mathcal{RE}}^{-1}$ and $\Xi(x) \triangleq e^x E_1(x)$. Here, $E_1(x) \triangleq \int_x^{\infty} e^{-t}t^{-1}dt$ is the exponential integral [44].

D. DF Scheme

In this scheme, $\mathcal{R}$ follows the conventional DF relaying scheme [10]. That is, $\mathcal{R}$ decodes the data from $\mathcal{S}$, re-encodes the decoded data and then forwards the encoded data to $\mathcal{D}$. The GSOP of the DF scheme is given by

$$
P_{out}^{(DF)} = \Pr\left\{ \left[\log_2 \left(\frac{1+\min\{\gamma_{\mathcal{SR}}, \gamma_{\mathcal{SD}}+\gamma_{\mathcal{RD}}\}}{1+\gamma_{\mathcal{SE}}+\gamma_{\mathcal{RE}}} \right) \right]^{+} < 2\theta R_s \right\}, \tag{31}
$$

where $\gamma_{\mathcal{RD}}$ and $\gamma_{\mathcal{RE}}$ are given by (28) and (29), respectively.[4] According to [32], $P_{out}^{(DF)}$ can be derived as

$$
\begin{aligned}
P_{out}^{(DF)} = &\frac{2^{-2\theta R_s}\bar{\gamma}_{\mathcal{SR}}\left[\Theta(\bar{\gamma}_{\mathcal{SE}})\Psi(\bar{\gamma}_{\mathcal{SE}}) - \Theta(\bar{\gamma}_{\mathcal{RE}})\Psi(\bar{\gamma}_{\mathcal{RE}})\right]}{(\bar{\gamma}_{\mathcal{RE}}-\bar{\gamma}_{\mathcal{SE}})(\bar{\gamma}_{\mathcal{RD}}-\bar{\gamma}_{\mathcal{SD}})} \\
&+ \frac{\Theta(\bar{\gamma}_{\mathcal{RE}}) - \Theta(\bar{\gamma}_{\mathcal{SE}})}{\bar{\gamma}_{\mathcal{RE}}-\bar{\gamma}_{\mathcal{SE}}},
\end{aligned} \tag{32}
$$

where

$$
\Theta(x) \triangleq \frac{x^2}{2^{-2\theta R_s}\bar{\gamma}_{\mathcal{SR}} + x} \exp\left(\frac{1-2^{-2\theta R_s}}{x}\right), \tag{33}
$$

$$
\begin{aligned}
\Psi(x) \triangleq &\frac{\bar{\gamma}_{\mathcal{SR}}}{x(1+\bar{\gamma}_{\mathcal{SR}}/\bar{\gamma}_{\mathcal{SD}}) + 2^{-2\theta R_s}\bar{\gamma}_{\mathcal{SR}}} \\
&- \frac{\bar{\gamma}_{\mathcal{SR}}}{x(1+\bar{\gamma}_{\mathcal{SR}}/\bar{\gamma}_{\mathcal{RD}}) + 2^{-2\theta R_s}\bar{\gamma}_{\mathcal{SR}}}.
\end{aligned} \tag{34}
$$

Remark 5 (*GSOP of DF Scheme*)**.** As noticed in Remark 4, the DF scheme is a special case of the PMF scheme when the SINRs of the links $\mathcal{R} \to \mathcal{D}$ and $\mathcal{R} \to \mathcal{E}$ are replaced by the SNRs of those links with no encryption and PNC operation. Indeed, the GSOP of the DF scheme in (32) can be derived from that of the PMF scheme in Theorem 1 by setting $\alpha = 1$ and $\beta = 0$ for the pdf of both $\gamma_{\mathcal{RD}}$ and $\gamma_{\mathcal{RE}}$ in (18).

Remark 6 (*Lower GSOP With PMF-Perfect Over DF Scheme*)**.** In the PMF-perfect scheme, given the fact that the message modification at $\mathcal{R}$ is perfectly shared between legitimate users, the SINR of the link $\mathcal{R} \to \mathcal{D}$ can be simplified to be the SNR of that link (see Remark 4), while the SINR of the link $\mathcal{R} \to \mathcal{E}$ is unchanged since $\mathcal{E}$ does not know the modification process at $\mathcal{R}$. Furthermore, it can be easily shown that $\Lambda_R|h_{\mathcal{RE}}|^2/\sigma^2 > \Lambda_R|h_{\mathcal{RE}}|^2\alpha^2/(\Lambda_R|h_{\mathcal{RE}}|^2\beta^2+\sigma^2), \forall\, 0 \le \alpha, \beta \le 1$. Therefore, from (14) and (31), it can be concluded that the PMF-perfect scheme achieves a lower GSOP for an

[4] Note that the SNRs of links $\mathcal{R} \to \mathcal{D}$ and $\mathcal{R} \to \mathcal{E}$ in the couterpart RT schemes are different from the SINRs of those links in the proposed PMF scheme (see (10) and (13)).

enhanced security compared to the DF scheme, which verifies the statement in Remark 1.[5]

E. MF Scheme

In MF scheme [34], $\mathcal{R}$ decodes the source message, modifies the message and then forwards the modified message to $\mathcal{D}$ with the assumption that the knowledge of the message modification process at $\mathcal{R}$ is perfectly shared between $\mathcal{R}$ and $\mathcal{D}$, and $\mathcal{E}$ is not able to utilise the modified message from $\mathcal{R}$. The GSOP of the MF scheme is thus given by

$$P_{out}^{(MF)} = \Pr\left\{\left[\log_2\left(\frac{1+\min\{\gamma_{\mathcal{SR}}, \gamma_{\mathcal{SD}}+\gamma_{\mathcal{RD}}\}}{1+\gamma_{\mathcal{SE}}}\right)\right]^+ < 2\theta R_s\right\}. \tag{35}$$

Following [34], $P_{out}^{(MF)}$ can be derived as

$$P_{out}^{(MF)} = 1 - \frac{\Phi(\bar{\gamma}_{\mathcal{RD}}) - \Phi(\bar{\gamma}_{\mathcal{SD}})}{\bar{\gamma}_{\mathcal{RD}} - \bar{\gamma}_{\mathcal{SD}}}, \tag{36}$$

where

$$\begin{aligned}\Phi(x) \triangleq &\left(1+\frac{x}{\bar{\gamma}_{\mathcal{SR}}}\right) e^{(1-2^{2\theta R_s})(\bar{\gamma}_{\mathcal{SR}}^{-1}+x^{-1})} \\ &\times \left(\frac{1}{\bar{\gamma}_{\mathcal{SR}}^{-1}+x^{-1}} - \frac{1}{2^{-2\theta R_s}\bar{\gamma}_{\mathcal{SE}}^{-1}+\bar{\gamma}_{\mathcal{SR}}^{-1}+x^{-1}}\right).\end{aligned} \tag{37}$$

Remark 7 (*GSOP of MF Scheme*)**.** From (31) and (35), it can be observed that the GSOP of the MF scheme can be deduced from that of the DF scheme given $\gamma_{\mathcal{RE}} = 0$. In fact, in the MF scheme, it is assumed that $\mathcal{E}$ can only decode the message from $\mathcal{S}$ in the first time slot, which implies that $\gamma_{\mathcal{RE}} = 0$. The MF scheme can be referred to as an 'ideal' DF scheme with $\gamma_{\mathcal{RE}} = 0$, and consequently a special case of our proposed PMF scheme (see Remark 2). The GSOP of the MF scheme in (36) can be therefore derived from that of the PMF scheme in (18) in Theorem 1 when $\alpha = 1$, $\beta = 0$ and $\gamma_{\mathcal{RE}} = 0$.

Remark 8 (*Much Lower GSOP With MF Scheme for an Ideal Case*)**.** From (14), (31) and (35), it can be easily seen that the MF scheme with the absence of the link $\mathcal{R} \to \mathcal{E}$ achieves the lowest GSOP compared to the PMF and DF schemes. Although such assumption in the MF scheme does not sound naturally in practice when the eavesdropper can overhear the message from all nodes, the GSOP of the MF scheme can be regarded as a performance benchmark providing the lower bound of the proposed PMF scheme.

Remark 9 (*Lower and Upper Bounds of the PMF Scheme*)**.** *It can be seen that* $\gamma_{\mathcal{RE}}^{(PMF)} \geq \gamma_{\mathcal{RE}}^{(MF)} = 0$ *and* $\gamma_{\mathcal{RE}}^{(PMF)} = \frac{\lambda_{\mathcal{R}}|h_{\mathcal{RE}}|^2\alpha^2}{\lambda_{\mathcal{R}}|h_{\mathcal{RE}}|^2\beta^2+\sigma_0^2} \leq \gamma_{\mathcal{RE}}^{(DF)} = \frac{\lambda_{\mathcal{R}}|h_{\mathcal{RE}}|^2}{\sigma_0^2}$ *when* $\alpha^2 \leq 1$*, and thus* $C_e^{(MF)} \leq C_e^{(PMF)} \leq C_e^{(DF)}$*. From* (5) *and* (6)*, we have* $P_{out}^{(MF)} \leq P_{out}^{(PMF)} \leq P_{out}^{(DF)}$*. This means that the GSOP of the PMF scheme is lower and upper bounded by that of the MF and DF schemes, respectively.*

[5]Note that the above claim in Remark 6 is not applied for the case of the PMF-imperfect scheme, which will be verified in the numerical results. Although no conclusion can be straightforwardly drawn for the PMF-imperfect scheme, it is worth claiming an enhanced security achieved with the proposed PMF scheme since the shared knowledge of signaling information between the legitimate users is normally guaranteed by a dedicated channel. For completeness, in this work, we consider both imperfectly and perfectly shared knowledge between legitimate users in the PMF scheme.

V. Opportunistic Secure Transmission Protocol for CWRNs

In a practical CWRN, it can be intuitively seen that the usage of relay node may be unnecessary if the link between source and relay and/or the link between relay and destination suffer(s) from severe fading and noise. In other words, DT scheme could be favourable over RT schemes given a dominant direct link of very high quality compared to relaying links. This accordingly raises a research problem in our considered system model to find out when the relay should be used to provide a higher secure communication over the DT scheme.

For clarity, let us consider the following example:

Example 1. The SNRs of the links in a CWRN (see Fig. 1) are set as $\bar{\gamma}_{\mathcal{SR}} = 12$ dB, $\bar{\gamma}_{\mathcal{RD}} = 10$ dB, $\bar{\gamma}_{\mathcal{SE}} = 5$ dB and $\bar{\gamma}_{\mathcal{RE}} = 7$ dB. Fig. 2 plots the GSOP of DT, DF, CJ, MF, PMF-perfect and PMF-imperfect schemes versus the target secrecy rate, i.e. R_s [b/s/Hz], with PNC coefficients $\{\alpha^2 = 0.7, \beta^2 = 0.3\}$, level of secrecy requirement $\theta = 1$ and with respect to two values of $\bar{\gamma}_{\mathcal{SD}} = \{0, 12\}$ dB. It can be seen that the GSOP of the DT scheme achieves the best performance when $\bar{\gamma}_{\mathcal{SD}} = 12$ dB, while there exists a crossing point between the GSOPs of the DT, DF, MF, PMF-perfect and PMF-imperfect schemes when $\bar{\gamma}_{\mathcal{SD}} = 0$ dB. For instance, the GSOP of the DT scheme intersects with that of the PMF-imperfect, DF, PMF-perfect, and MF schemes when $R_s = R_{s,1} = 0.07$ b/s/Hz, $R_s = R_{s,2} = 0.66$ b/s/Hz, $R_s = R_{s,3} = 1.2$ b/s/Hz and $R_s = R_{s,4} = 1.8$ b/s/Hz, respectively. We have the following observations when $\bar{\gamma}_{\mathcal{SD}} = 0$ dB:

i) If $R_s < R_{s,1}$, then $P_{out}^{(DT)} > P_{out}^{(PMF-imperfect)} > P_{out}^{(DF)} > P_{out}^{(PMF-perfect)} > P_{out}^{(MF)}$;
ii) If $R_{s,1} \leqslant R_s < R_{s,2}$, then $P_{out}^{(PMF-imperfect)} > P_{out}^{(DT)} > P_{out}^{(DF)} > P_{out}^{(PMF-perfect)} > P_{out}^{(MF)}$;
ii) If $R_{s,2} \leqslant R_s < R_{s,3}$, then $P_{out}^{(PMF-imperfect)} > P_{out}^{(DF)} > P_{out}^{(DT)} > P_{out}^{(PMF-perfect)} > P_{out}^{(MF)}$;
iv) If $R_{s,3} \leqslant R_s < R_{s,4}$, then $P_{out}^{(PMF-imperfect)} > P_{out}^{(DF)} > P_{out}^{(PMF-perfect)} > P_{out}^{(DT)} > P_{out}^{(MF)}$;
iv) If $R_s \geqslant R_{s,4}$, then $P_{out}^{(PMF-imperfect)} > P_{out}^{(DF)} > P_{out}^{(PMF-perfect)} > P_{out}^{(MF)} > P_{out}^{(DT)}$.

This accordingly reflects that the relay may be helpful in providing a lower GSOP at a specific range of the target secrecy rate, while the DT scheme could provide a better secrecy performance without any support of the relay.

Inspired from the above observations in Example 1, we introduce an optimisation problem as follows

$$\min_{X \in \{DT, RT\}} P_{out}^{(X)}, \tag{38}$$

where $P_{out}^{(X)}$ of various schemes is derived in Section III.

The optimisation problem in (38) aims to find the best transmission strategies, in terms of lowest GSOP, amongst the DT scheme and various RT schemes, i.e. DF, MF and

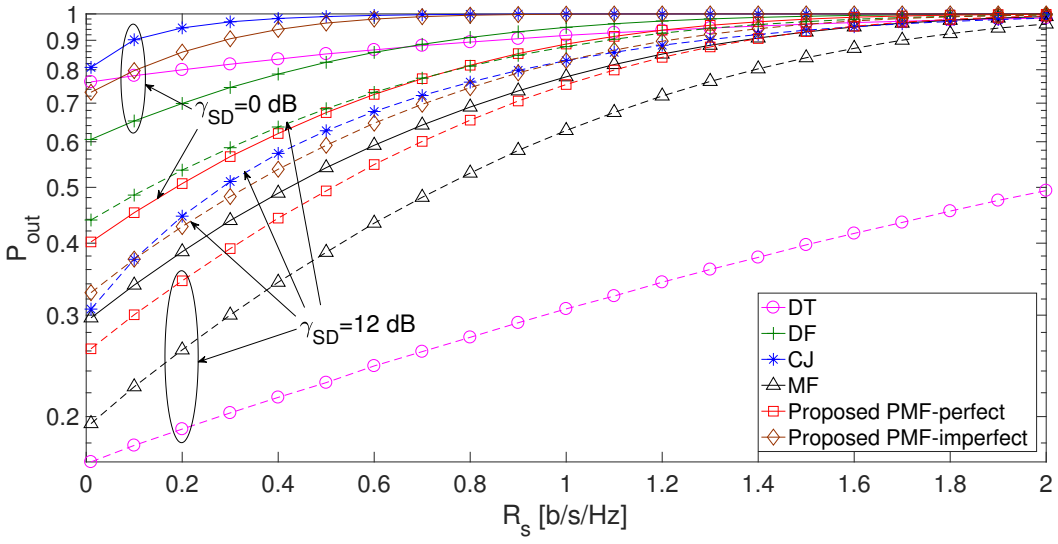

Fig. 2: Illustration of threshold of R_s for selecting appropriate schemes for secure communications.

PMF. Considering the GSOP as a function of the target secrecy rate, i.e. R_s, Example 1 suggests that there may exist crossing points or intersections between the GSOP curves. Having in mind that an intersection between two GSOP curves identifies their different trends, one can easily find the lower GSOP curve at a given R_s. Therefore, in order to avoid an exhaustive search when solving (38), it is crucial to find the existence conditions of these crossing points. Let us first introduce the following propositions:

Proposition 1. *Given two non-negative increasing functions* $f(x)$ *and* $g(x)$ *with* $\frac{df(x)}{dx} > \frac{dg(x)}{dx} > 0$, *then* $\exists! x' > 0 : f(x') = g(x')$ *if and only if* $f(0) < g(0)$.

Proof. See Appendix C. □

Proposition 2. *Given three non-negative increasing functions* $f(x)$, $g(x)$ *and* $h(x)$ *having* $\frac{df(x)}{dx} > \frac{dg(x)}{dx} > \frac{dh(x)}{dx} > 0$, *if* $f(0) > g(0)$ *and* $\exists! x_1 > 0 : f(x_1) = h(x_1)$, *then* $\exists! x_2 > 0 : g(x_2) = h(x_2)$.

Proof. From Proposition 1, given $\frac{df(x)}{dx} > \frac{dh(x)}{dx} > 0$, if $\exists! x_1 > 0 : f(x_1) = h(x_1)$, then we have $f(0) < h(0)$, and thus $h(0) > g(0)$. Accordingly, it can be deduced that $\exists! x_2 > 0 : g(x_2) = h(x_2)$ since $\frac{dg(x)}{dx} > \frac{dh(x)}{dx} > 0$ and $g(0) < h(0)$. □

The findings in Propositions 1 and 2 verify the crossing points of the GSOP curves of the DT, DF, MF and the proposed PMF in Fig. 2 at different values of R_s. For simplicity, let us consider DT and MF scheme as an exemplary RT scheme due to its tractability with the GSOP derived in the previous section, while the other RT schemes will be validated through numerical results in Section V. The conditions of the intersection between two GSOP curves of the DT and RT schemes are determined as in the following Theorem 2.

Theorem 2. *On the subject of target secrecy rate, i.e.* R_s, *there exists a single crossing point of two GSOP curves for the DT and RT schemes if* $\bar{\gamma}_{\mathcal{SD}}\bar{\gamma}_{\mathcal{SE}} < \bar{\gamma}^2_{\mathcal{SR}}$, $\bar{\gamma}_{\mathcal{SD}} < \sqrt{\bar{\gamma}_{\mathcal{SR}}\bar{\gamma}_{\mathcal{SE}}/2}$ *and* $\bar{\gamma}_{\mathcal{SD}} < \sqrt{\bar{\gamma}_{\mathcal{SR}}\bar{\gamma}_{\mathcal{RD}}/2}$. *That is* $\exists! R'_s > 0 : P_{out}^{(DT)}(R'_s) = P_{out}^{(RT)}(R'_s)$

Proof. See Appendix D. □

For convenience, let Ω_{cross} denote the set of conditions for the crossover of DT and RT schemes in Theorem 2, i.e.

$$\begin{aligned}\Omega_{cross} =&\{(\bar{\gamma}_{\mathcal{SD}}\bar{\gamma}_{\mathcal{SE}} < \bar{\gamma}^2_{\mathcal{SR}}) \wedge (\bar{\gamma}_{\mathcal{SD}} < \sqrt{\bar{\gamma}_{\mathcal{SR}}\bar{\gamma}_{\mathcal{SE}}/2}) \\ &\wedge (\bar{\gamma}_{\mathcal{SD}} < \sqrt{\bar{\gamma}_{\mathcal{SR}}\bar{\gamma}_{\mathcal{RD}}/2})\}.\end{aligned} \tag{39}$$

We have the following observation:

Remark 10 (*Existence of a Secrecy Rate Threshold (SRT) for Opportunistic Secure RT Protocol*)**.** From Theorem 2, if the channel quality satisfies the condition set Ω_{cross} in (39), then there exists a SRT, i.e. R_{th}, which is the crossing point between the GSOPs of DT and RT schemes. Specifically, it can be deduced that

$$\begin{cases} P_{out}^{(DT)}(R_s) > P_{out}^{(RT)}(R_s) & \text{if } R_s < R_{th} \\ P_{out}^{(DT)}(R_s) \leq P_{out}^{(RT)}(R_s) & \text{if } R_s \geq R_{th} \end{cases} \tag{40}$$

This accordingly means that we should select the RT scheme for a lower GSOP if the target secrecy rate is smaller than the SRT, while the DT scheme is preferable to achieve a higher target secrecy rate. Also, notice that if the SRT does not exist, i.e. the condition set Ω_{cross} is not satisfied, then the DT scheme should be selected as $P_{out}^{(DT)}(R_s) < P_{out}^{(RT)}(R_s)$, e.g. see Fig. 2 in Example 1 when $\gamma_{\mathcal{SD}} = 12$ dB.

Therefore, given Ω_{cross}, solving the optimisation problem (38) is turned into finding SRT between DT and each of RT schemes, i.e. DF, MF and PMF, as follows:

$$R_{th} = \left\{ R_s \middle| P_{out}^{(DT)}(R_s) = P_{out}^{(RT)}(R_s) \cap \Omega_{cross} \right\}. \tag{41}$$

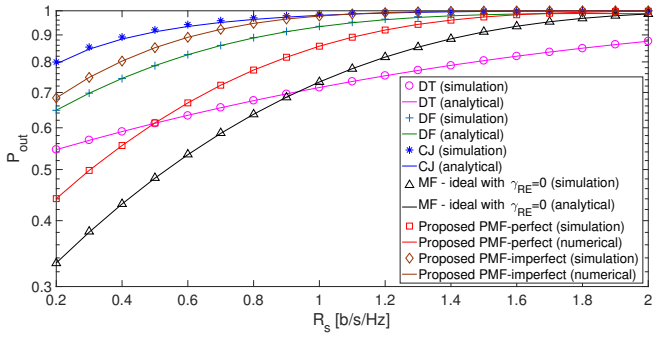

Fig. 3: GSOP versus target secrecy rate.

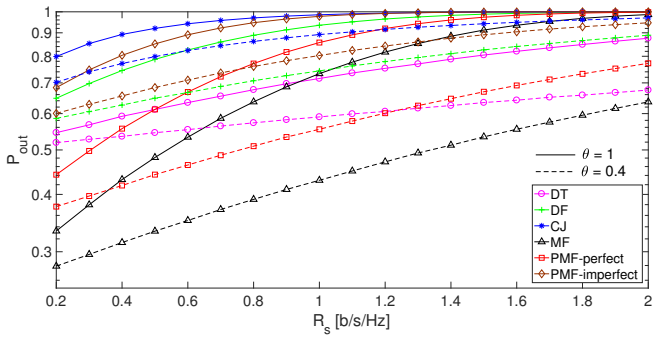

Fig. 4: GSOP versus target secrecy rate with respect to different secrecy requirements.

Using the derived GSOPs of various schemes in Section IV, R_{th} can be found via a simple numerical method and the optimal scheme can be opportunistically determined as in Remark 10.

VI. Numerical Results

In this section, we first illustrate the GSOP achieved with the proposed PMF scheme in CWRNs. In order to verify the effectiveness of the proposed PMF, the performance of DT [40], DF [32], CJ [13] and MF [34] are provided for comparison. The results are obtained with MATLAB under different scenarios of the wireless channel quality and the target secrecy rate. We then present the findings of SRTs for opportunistic secure RT protocol with respect to the quality of various links.

A. GSOP of DT & various RT Schemes

1) GSOP versus Target Secrecy Rate: Figure 3 plots the GSOP of various schemes as a function of the target secrecy rate, i.e. R_s. The SNRs of all links are set as $\bar{\gamma}_{\mathcal{SR}} = 12$ dB, $\bar{\gamma}_{\mathcal{RD}} = 10$ dB, $\bar{\gamma}_{\mathcal{SD}} = 5$ dB, $\bar{\gamma}_{\mathcal{RE}} = 7$ dB and $\bar{\gamma}_{\mathcal{SE}} = 5$ dB. Note that the eavesdropper can be a neighbouring node of the relay and destination nodes, and thus the eavesdropping links can have approximately the same SNR values as those of the direct and relaying links. The PNC coefficients and the level of secrecy requirement are set as $\{\alpha^2 = 0.7, \beta^2 = 0.3\}$ and $\theta = 1$, respectively. In Fig. 3, as noticed in the proof of Theorem 2, it can be seen that the GSOP increases over R_s and the gradient of the GSOP of the RT schemes is higher than that of the DT scheme. The PMF-perfect scheme is shown to achieve an improved GSOP performance over the DF, CJ and PMF-imperfect scheme, while the DT scheme achieves a better performance at high R_s. This accordingly verifies the statement in Remark 6 regarding the lower GSOP achieved with the PMF-perfect over the DF scheme, and also confirms the existence of the SRTs as stated in Remark 10. Additionally, it can be observed that the MF scheme achieves a lower GSOP compared to the proposed PMF-perfect scheme due to the neglect of the link $\mathcal{R} \to \mathcal{E}$. This is indeed regarded as the lower bound of the proposed PMF scheme, which according to Remark 8 the MF scheme is an ideal case though unnatural.[6] Moreover, the numerical and analytical results in Section III are shown to be consistent with the simulation results.

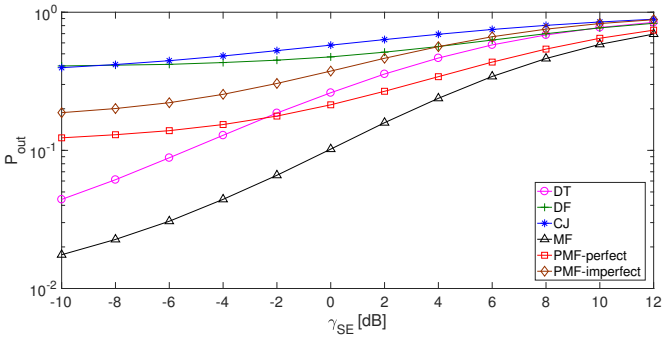

Fig. 5: GSOP versus SNR of the link $\mathcal{S} \to \mathcal{E}$.

Considering different secrecy requirements, Fig. 4 illustrates the GSOP versus target secrecy rate, i.e. R_s, with respect to different levels of secrecy requirement, i.e. θ. Specifically, two scenarios of $\theta = 1$ and $\theta = 0.4$ are considered, while the other parameters are similarly set as in Fig. 3. It can be observed in Fig. 4 that a relaxed secrecy requirement with a lower θ results in a lower secrecy outage and the GSOP is also shown to increase for all cases as the target secrecy rate increases. For simplicity, in the rest of this section, let us consider the scenario when $\theta = 1$.

2) Impacts of Eavesdropper Links: Figures 5 and 6 sequentially plot the GSOP of various schemes for secure CWRN as a function of the average SNRs of the links $\mathcal{S} \to \mathcal{E}$, i.e. $\bar{\gamma}_{\mathcal{SE}}$, and $\mathcal{R} \to \mathcal{E}$, i.e. $\bar{\gamma}_{\mathcal{RE}}$, respectively. In Fig. 5, the range of $\bar{\gamma}_{\mathcal{SE}}$ is selected to cover -10 dB to 12 dB and $\bar{\gamma}_{\mathcal{RE}} = 7$ dB, while $\bar{\gamma}_{\mathcal{RE}}$ is in the range from -10 to 10 dB in Fig. 6 and $\bar{\gamma}_{\mathcal{SE}} = 5$ dB. In both figures, the SNRs of other channels are set as $\bar{\gamma}_{\mathcal{SR}} = 12$ dB, $\bar{\gamma}_{\mathcal{SD}} = 5$ dB, $\bar{\gamma}_{\mathcal{RD}} = 10$ dB, the target secrecy rate is $R_s = 0.1$ b/s/Hz and the PNC coefficients are $\{\alpha^2 = 0.7, \beta^2 = 0.3\}$.

As shown in Fig. 5, a higher $\bar{\gamma}_{\mathcal{SE}}$ causes a higher GSOP as the eavesdropper can more reliably decode the source message.

[6]Note that the MF scheme always provides a lower GSOP compared to the DF and PMF schemes. Also, the GSOP of the PMF-imperfect scheme is always higher than that of the PMF-perfect scheme. Therefore, in what follows, we only discuss the PMF-perfect scheme (say PMF in short) with respect to DT, DF and CJ schemes, while the performance of the PMF-imperfect and MF schemes is only plotted for completeness, but not repeatedly interpreted for their reasoning.

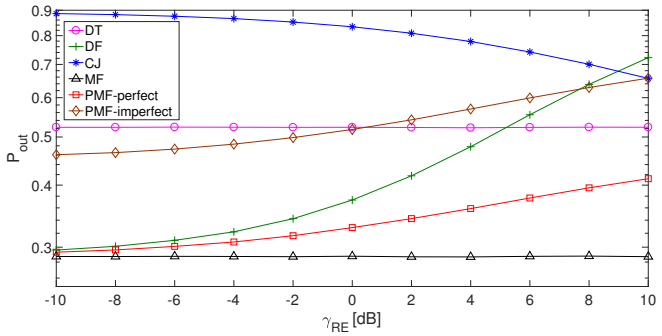

Fig. 6: GSOP versus SNR of the link $\mathcal{R} \to \mathcal{E}$.

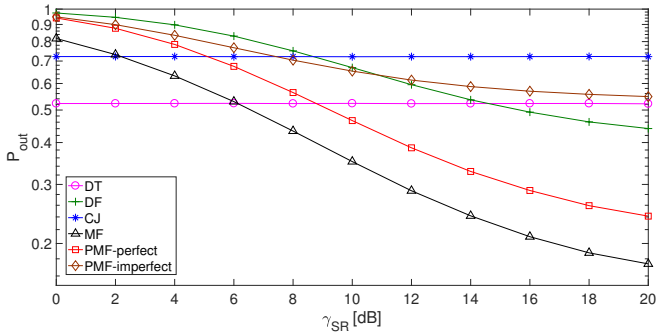

Fig. 7: GSOP versus SNR of the link $\mathcal{S} \to \mathcal{R}$.

It can be observed that the proposed PMF scheme achieves a lower GSOP compared to the DF and CJ schemes over the whole range of $\bar{\gamma}_{\mathcal{SE}}$ and performs better than the DT scheme at high $\bar{\gamma}_{\mathcal{SE}}$, while the DT scheme achieves a better performance at low $\bar{\gamma}_{\mathcal{SE}}$ which is corresponding to the scenario when $\mathcal{E}$ can not reliably decode the message from $\mathcal{S}$. This again verifies our statements in Remarks 1 and 6 regarding the improved security with the proposed PMF scheme as well as confirming Remark 10 in respect of the SRTs between the DT and RT schemes. A similar observation can be made in Fig. 6 where the proposed PMF is shown to achieve a better performance compared to the DT, DF and CJ schemes.

3) Impacts of Relaying Links: In CWRN, both links $\mathcal{S} \to \mathcal{R}$ and $\mathcal{R} \to \mathcal{D}$ need to be considered for reliable relaying. Figs. 7 and 8 plot GSOP of DT and various RT schemes including DF, CJ, MF, PMF-imperfect and PMF-perfect schemes

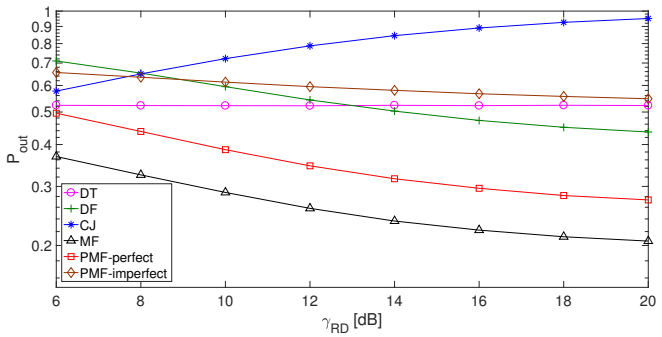

Fig. 8: GSOP versus SNR of the link $\mathcal{R} \to \mathcal{D}$.

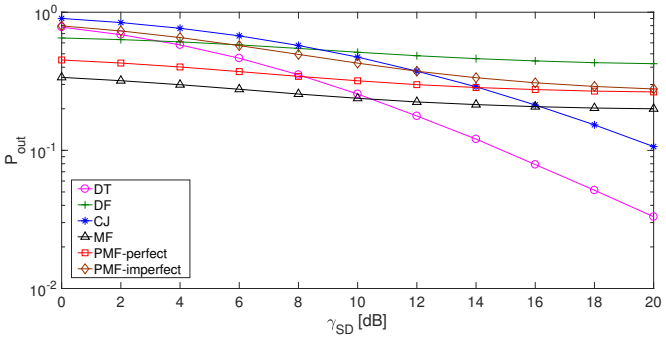

Fig. 9: GSOP versus SNR of the link $\mathcal{S} \to \mathcal{D}$.

versus $\bar{\gamma}_{\mathcal{SR}}$ and $\bar{\gamma}_{\mathcal{RD}}$, respectively. It is assumed that $\bar{\gamma}_{\mathcal{RD}} = 10$ dB in Fig. 7 and $\bar{\gamma}_{\mathcal{SR}} = 12$ dB in Fig. 8. In both figures, the SNRs of other channels are set as $\bar{\gamma}_{\mathcal{SD}} = 5$ dB, $\bar{\gamma}_{\mathcal{RE}} = 7$ dB and $\bar{\gamma}_{\mathcal{SE}} = 5$ dB. Similarly, the target secrecy rate is $R_s = 0.1$ b/s/Hz and the PNC coefficients are $\{\alpha^2 = 0.7, \beta^2 = 0.3\}$. It can be observed in both Figs. 7 and 8 that a lower GSOP is achieved with the proposed PMF scheme compared to the DF scheme and also shown to be better than the DT scheme at high $\bar{\gamma}_{\mathcal{SR}}$. In fact, the high-quality link $\mathcal{S} \to \mathcal{R}$ provides a reliable relaying, and thus $\mathcal{R}$ can help to enhance the security in CWRN. At low $\bar{\gamma}_{\mathcal{SR}}$, e.g. $\bar{\gamma}_{\mathcal{SR}} < 6$ dB, $\mathcal{R}$ may not be able to reliably decode the data message from $\mathcal{S}$ and thus the DT scheme is beneficial in this case. Additionally, in Fig. 7, the performance of the DT and CJ schemes is shown to be independent of $\bar{\gamma}_{\mathcal{SR}}$ as there is no relay involved in the DT scheme and the jamming process at $\mathcal{R}$ in the CJ scheme does not rely on the reliability of the link $\mathcal{S} \to \mathcal{R}$. It can also be noticed in Fig. 8 that the CJ scheme even has a poorer GSOP performance when $\bar{\gamma}_{\mathcal{RD}}$ increases since the jamming signals at $\mathcal{R}$ also causes a considerable harm on the message decoding at $\mathcal{D}$, especially in a very good channel condition.

4) Impacts of Direct Link: Taking into account the direct link $\mathcal{S} \to \mathcal{D}$ in CWRN, Fig. 9 plots the GSOP of various schemes as a function of $\bar{\gamma}_{\mathcal{SD}}$. The SNRs of other links are $\bar{\gamma}_{\mathcal{SR}} = 12$ dB, $\bar{\gamma}_{\mathcal{RD}} = 10$ dB, $\bar{\gamma}_{\mathcal{RE}} = 7$ dB and $\bar{\gamma}_{\mathcal{SE}} = 5$ dB. Similarly, the target secrecy rate and the PNC coefficients are $R_s = 0.1$ b/s/Hz and $\{\alpha^2 = 0.7, \beta^2 = 0.3\}$. It can be observed in Fig. 9 that the proposed PMF scheme achieves a lower GSOP than the DF scheme. The PMF is also shown to be better than the DT and CJ schemes at low $\bar{\gamma}_{\mathcal{SD}}$. However, at high $\bar{\gamma}_{\mathcal{SD}}$, the DT scheme is shown to be the best scheme as the usage of $\mathcal{R}$ is not necessary in this case, even degrading the performance. This again verifies the statement in Remark 10 regarding the necessity of determining the SRT for opportunistic secure transmission scheme in the CWRN.

B. SRTs for Opportunistic Secure RT Protocol

1) SRTs w.r.t. Quality of Relaying Links: Considering the impacts of the links $\mathcal{S} \to \mathcal{R}$ and $\mathcal{R} \to \mathcal{D}$ on determining SRT for opportunistic secure communication protocol, Figs. 10 and 11 plot the SRT, i.e. R_{th}, of DF, MF and the proposed PMF schemes as a function of $\bar{\gamma}_{\mathcal{SR}}$ and $\bar{\gamma}_{\mathcal{RD}}$, respectively. The SNRs of other channel links are similarly set as in Fig. 7

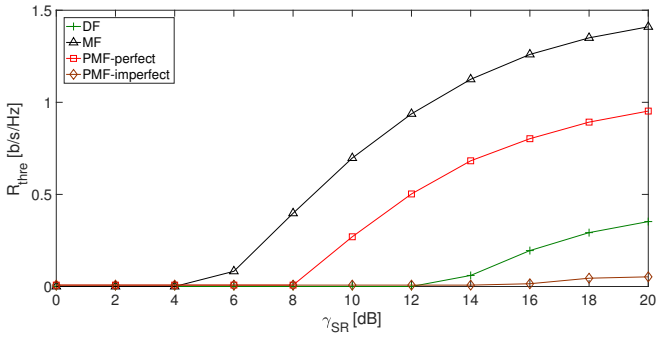

Fig. 10: SRT of various RT schemes versus $\bar{\gamma}_{\mathcal{SR}}$.

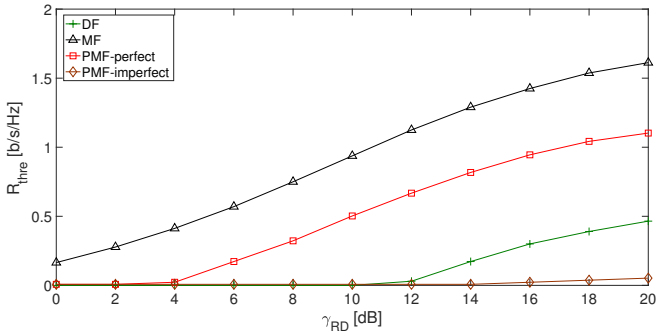

Fig. 11: SRT of various RT schemes versus $\bar{\gamma}_{\mathcal{RD}}$.

and Fig. 8. It can be observed in both figures that $R_{th} = 0$ at low $\bar{\gamma}_{\mathcal{SR}}$. In fact, when $\bar{\gamma}_{\mathcal{SR}}$ is low, the condition set in Theorem 2, i.e. Ω_{cross} in (39), is not satisfied, and thus there do not exist any crossing points between the GSOP curves of the DT scheme and other schemes. This means that the DT scheme is optimal in the low-SNR regime of the link $\mathcal{S} \to \mathcal{R}$ (see Remark 10). It can also be observed that R_{th} increases as either $\bar{\gamma}_{\mathcal{SR}}$ or $\bar{\gamma}_{\mathcal{RD}}$ increases. This is due to the fact that a higher SNR of the relaying links results in a better GSOP performance of the RT schemes, and thus, as shown in Proposition 2, a higher R_{th} is obtained.

2) SRTs w.r.t. Quality of Direct Link: Taking into account the direct link $\mathcal{S} \to \mathcal{D}$, Fig. 12 plots R_{th} of various RT schemes as a function of $\bar{\gamma}_{\mathcal{SD}}$. The range of $\bar{\gamma}_{\mathcal{SD}}$ is assumed to vary from 0 to 10 dB and the SNRs of other channel links are set as in Fig. 9. Different from Figs. 10 and 11, it can be observed in Fig. 12 that the increase of $\bar{\gamma}_{\mathcal{SD}}$ results in a lower R_{th} and such decrease approaches 0 as $\bar{\gamma}_{\mathcal{SD}} \geq 10$ dB. This accordingly means that if the direct link is of high quality, then the DT scheme is more beneficial than the RT schemes with a lower GSOP and also a lower R_{th}. In fact, at high $\bar{\gamma}_{\mathcal{SD}}$ dB, the condition set Ω_{cross} is not satisfied (see (39)), and hence, as noticed in Remark 10 with an illustration in Example 1, the DT scheme is optimal in the high-SNR regime of the direct link.

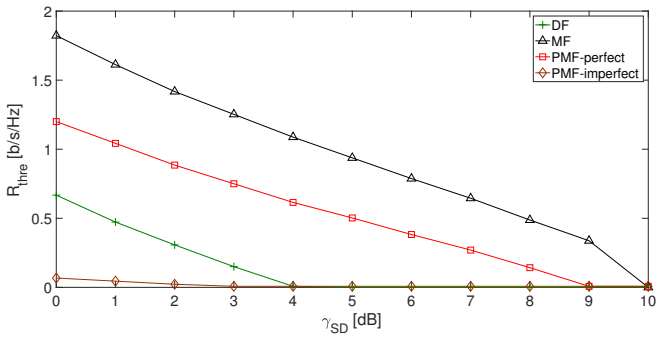

Fig. 12: SRT of various RT schemes versus $\bar{\gamma}_{\mathcal{SD}}$.

VII. Conclusions

In this paper, an efficient PMF scheme has been proposed for secure CWRNs to cope with the scenario when the eavesdropper can overhear the message from both the source and the relay, and also the imperfectly shared knowledge between the relay and destination as in the conventional MF scheme. By employing PNC at the relay with encrypted key, the proposed scheme has been shown to provide a higher security compared to the conventional DF and CJ schemes with respect to various channel conditions and target secrecy rates. Additionally, the GSOP of the PMF scheme has been derived, which is a general form of the DF and MF schemes. The PMF scheme is shown to provide higher security compared to the DF scheme while approaching the MF scheme of which the GSOP is a lower bound in an ideal case of no communication link between the relay and the eavesdropper. Furthermore, we have proposed an opportunistic secure transmission protocol by finding the SRTs for determining the optimal scheme with or without the assistance of the relay. Depending on the quality of channel links, the conditions for the existence of the SRTs have been derived. It is shown that the SRTs increase as the SNR of either source-relay or relay-destination link increases, while the increase of the SNR of source-destination link results in lower SRTs. For future work, we will investigate the design of the PNC coefficients at the relay with respect to the channel gains of different links. Untrusted relay channels will be also taken into account for the scenario when the relay as a third party is not allowed to decode the confidential message.

Appendix A
Proof of Lemma 1

Given $Y = \dfrac{a^2 X}{b^2 X + 1}$ and $X = c|Z|^2$ where c is a positive constant, it can be deduced that $a^2 \geq b^2 Y$. The cdf of Y can be computed by [45]

$$F_Y(y) = \Pr\{Y \leqslant y\} = \Pr\left\{X \leqslant \frac{y}{a^2 - b^2 y}\right\}. \quad (42)$$

Note that the pdf and cdf of X are given by

$$f_X(x) = \frac{1}{c}\exp\left(-\frac{x}{c}\right), \quad (43)$$

$$F_X(x) = Pr\{X \leqslant x\} = \int_0^x f_X(t)dt = 1 - \exp\left(-\frac{x}{c}\right), \quad (44)$$

respectively. Substituting (44) into (42), we have

$$F_Y(y) = F_X\left(\frac{y}{a^2 - b^2 y}\right) = 1 - \exp\left(-\frac{y}{c(a^2 - b^2 y)}\right) \quad (45)$$

The pdf of Y can be therefore obtained by

$$f_Y(y) = \frac{dF_Y(y)}{dy} = \frac{a^2}{c(a^2-b^2y)^2} \exp\left[-\frac{y}{c(a^2-b^2y)}\right]. \quad (46)$$

APPENDIX B
PROOF OF THEOREM 1

For brevity, let $X = \gamma_{\mathcal{SR}}$, $Y = \gamma_{\mathcal{SD}}$, $Z = \gamma_{\mathcal{RD}}$, $U = \gamma_{\mathcal{SE}}$ and $V = \gamma_{\mathcal{RE}}$. We can rewrite (14) as

$$P_{out}^{(PMF)} = \Pr\left\{\left[\log_2\left(\frac{1+\min\{X, Y+Z\}}{1+U+V}\right)\right]^+ < 2\theta R_s\right\}. \quad (47)$$

Note that the secure communication is possible with a positive secrecy capacity if the legitimate links, including the direct and/or relaying links, have higher channel gains over the eavesdropper links. In order to prevent the secrecy outage from always happening, it is assumed that $\min\{X, Y+Z\} > U+V$. From (47), we have

$$\begin{aligned} P_{out}^{(PMF)} &= \Pr\left\{\log_2\left(\frac{1+\min\{X, Y+Z\}}{1+U+V}\right) < 2\theta R_s\right\} \\ &= \Pr\left\{2^{-2R_s}(1+\min\{X, Y+Z\}) - 1 < U+V\right\}, \end{aligned} \quad (48)$$

Considering two scenarios of $X \leqslant Y+Z$ and $X > Y+Z$, (48) can be rewritten by (49) (see the top of next page).

Deriving P_1 and P_2 in (49), it can be observed that, if $X \leqslant \min\{Y, 2^{2\theta R_s}-1\}$, then $\Pr\{2^{-2\theta R_s}(1+X)-1 < U+V < X\} = 1$ and $\Pr\{X \leqslant Y+Z\} = 1$ since $U+V \geqslant 0$ and $Z \geqslant 0$. This means $P_1 = 1$ and $P_2 = 0$, i. e. $P_{out}^{(PMF)} = 1$ (outage occurs). Similarly, if $Y+Z \leqslant \min\{X, 2^{2\theta R_s}-1\}$, then $\Pr\{2^{-2\theta R_s}(1+Y+Z)-1 < U+V < Y+Z\} = 1$ and $\Pr\{X > Y+Z\} = 1$ since $U+V \geqslant 0$, and thus outage happens. Therefore, in order to avoid the outage, by considering all these above conditions, we can arrive at (50) and (51) (see the top of next page).

For simplicity, let us define

$$I_1(x) \triangleq \int_0^x f_U(u) \int_{2^{-2\theta R_s}(1+x)-1-u}^{x-u} f_V(v)\, dv\, du, \quad (52)$$

$$I_2(x) \triangleq \int_0^x f_U(u) \int_0^{x-u} f_V(v)\, dv\, du. \quad (53)$$

Substituting (50) and (51) into (49) with $I_1(x)$ and $I_2(x)$, the theorem is proved.

APPENDIX C
PROOF OF PROPOSITION 1

From $\frac{df(x)}{dx} > \frac{dg(x)}{dx} > 0$, there exist $x_1 > 0$ and $x_2 > 0$ such that

$$\frac{f(x_1)-f(0)}{x_1} > \frac{g(x_2)-g(0)}{x_2}. \quad (54)$$

If $f(0) < g(0)$, then there exists a crossing point $x' = x_1 = x_2 > 0$ such that $f(x') = g(x')$ and thus $(f(x')-f(0))/x' > (g(x')-g(0))/x'$ satisfying (54). Conversely, if there exists a crossing point $x' = x_1 = x_2 > 0$ satisfying (54), then we can easily deduce that $f(0) < g(0)$.

Proof of uniqueness: Let us assume that there exists $0 < x'' \neq x'$ satisfying $f(x'') = g(x'')$ and $f(x') = g(x')$. We have

$$\frac{f(x'')-f(x')}{x''-x'} = \frac{g(x'')-g(x')}{x''-x'}, \quad (55)$$

which contradicts the fact that $\frac{df(x)}{dx} > \frac{dg(x)}{dx}$.

Therefore, we can conclude that $\exists! x' > 0 : f(x') = g(x')$ if and only if $f(0) < g(0)$.

APPENDIX D
PROOF OF THEOREM 2

In the DT protocol, as $R_s \to 0$, it can be observed from (26) that

$$P_{out}^{(DT)} \to \frac{\bar{\gamma}_{\mathcal{SE}}}{\bar{\gamma}_{\mathcal{SD}} + \bar{\gamma}_{\mathcal{SE}}} \triangleq P_0^{(DT)}. \quad (56)$$

In the RT protocol, as $R_s \to 0$, $\Phi(x)$ in (37) approaches

$$\begin{aligned} \Phi(x) &\to \left(1+\frac{x}{\bar{\gamma}_{\mathcal{SR}}}\right)\left(\frac{1}{\bar{\gamma}_{\mathcal{SR}}^{-1}+x^{-1}} - \frac{1}{\bar{\gamma}_{\mathcal{SE}}^{-1}+\bar{\gamma}_{\mathcal{SR}}^{-1}+x^{-1}}\right) \\ &= \frac{x^2\bar{\gamma}_{\mathcal{SR}}}{x\bar{\gamma}_{\mathcal{SR}} + x\bar{\gamma}_{\mathcal{SE}} + \bar{\gamma}_{\mathcal{SR}}\bar{\gamma}_{\mathcal{SE}}}. \end{aligned} \quad (57)$$

Substituting (57) into (36), the limit of $P_{out}^{(RT)}$ can be obtained by (58) (see the top of next page).

Denote $\Delta = P_0^{(RT)} - P_0^{(DT)}$. Solving $\Delta < 0$, after some mathematical manipulations, we obtain the condition of the channel quality of various links as in (59) (see the top of next page). It can be seen that, if $\bar{\gamma}_{\mathcal{SD}}\bar{\gamma}_{\mathcal{SE}} < \bar{\gamma}_{\mathcal{SR}}^2$, $\bar{\gamma}_{\mathcal{SD}} < \sqrt{\bar{\gamma}_{\mathcal{SR}}\bar{\gamma}_{\mathcal{SE}}/2}$ and $\bar{\gamma}_{\mathcal{SD}} < \sqrt{\bar{\gamma}_{\mathcal{SR}}\bar{\gamma}_{\mathcal{RD}}/2}$, then $\Delta < 0$, i.e. $P_0^{(RT)} < P_0^{(DT)}$. Additionally, as in the conventional relaying scheme, the gradient of the GSOP performance of the RT scheme is higher than that of the DT scheme and the GSOP of both schemes increases as a function of the target secrecy rate, i.e. $\frac{dP_{out}^{(RT)}}{dR_s} > \frac{dP_{out}^{(DT)}}{dR_s} > 0$. Therefore, from Proposition 1, we can conclude that $\exists! R_s' > 0 : P_{out}^{(DT)}(R_s') = P_{out}^{(RT)}(R_s')$.

REFERENCES

[1] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proceedings of the National Academy of Sciences*, vol. 114, no. 1, pp. 19–26, 2017.

[2] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 16–28, Sep. 2013.

[3] L. Fan, X. Lei, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Secure multiuser communications in multiple amplify-and-forward relay networks," *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3299–3310, Sept. 2014.

[4] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: state of the art and beyond," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 32–39, Dec. 2015.

[5] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying with cochannel interference," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1494–1505, Dec. 2016.

[6] A. A. Nasir, H. D. Tuan, T. Q. Duong, and H. V. Poor, "Secure and energy-efficient beamforming for simultaneous information and energy transfer," *IEEE Trans. Wireless Commun.*, vol. 16, no. 11, pp. 7523–7537, Nov. 2017.

$$P_{out}^{(PMF)} = \underbrace{\Pr\{2^{-2\theta R_s}(1+X)-1<U+V<X\}\Pr\{X\leqslant Y+Z\}}_{\triangleq P_1} + \underbrace{\Pr\{2^{-2\theta R_s}(1+Y+Z)-1<U+V<Y+Z\}\Pr\{X>Y+Z\}}_{\triangleq P_2}. \tag{49}$$

$$\begin{aligned}P_1 =& \int_{2^{2\theta R_s}-1}^{\infty} f_Y(y)\int_{y}^{\infty} f_X(x)\int_{x-y}^{\infty} f_Z(z)\int_{0}^{x} f_U(u)\int_{2^{-2\theta R_s}(1+x)-1-u}^{x-u} f_V(v)\,dv\,du\,dz\,dx\,dy\\ &+\int_{2^{2\theta R_s}-1}^{\infty} f_X(x)\int_{x}^{\infty} f_Y(y)\int_{0}^{x} f_U(u)\int_{2^{-2\theta R_s}(1+x)-1-u}^{x-u} f_V(v)\,dv\,du\,dy\,dx\\ &+\int_{0}^{2^{2\theta R_s}-1} f_Y(y)\int_{y}^{2^{2\theta R_s}-1} f_X(x)\int_{x-y}^{\infty} f_Z(z)\int_{0}^{x} f_U(u)\int_{0}^{x-u} f_V(v)\,dv\,du\,dz\,dx\,dy\\ &+\int_{0}^{2^{2\theta R_s}-1} f_Y(y)\int_{2^{2\theta R_s}-1}^{\infty} f_X(x)\int_{x-y}^{\infty} f_Z(z)\int_{0}^{x} f_U(u)\int_{2^{-2\theta R_s}(1+x)-1-u}^{x-u} f_V(v)\,dv\,du\,dz\,dx\,dy,\end{aligned} \tag{50}$$

$$P_2 = \int_{2^{2\theta R_s}-1}^{\infty} f_X(x)\int_{2^{2\theta R_s}-1}^{x} f_Y(y)\int_{2^{2\theta R_s}-1-y}^{x-y} f_Z(z)\int_{0}^{y+z} f_U(u)\int_{2^{-2\theta R_s}(1+y+z)-1-u}^{y+z-u} f_V(v)\,dv\,du\,dz\,dy\,dx. \tag{51}$$

$$\begin{aligned}P_{out}^{(RT)} \to& 1-\frac{\dfrac{\bar\gamma_{\mathcal{RD}}^2\bar\gamma_{\mathcal{SR}}}{\bar\gamma_{\mathcal{RD}}\bar\gamma_{\mathcal{SR}}+\bar\gamma_{\mathcal{RD}}\bar\gamma_{\mathcal{SE}}+\bar\gamma_{\mathcal{SR}}\bar\gamma_{\mathcal{SE}}}-\dfrac{\bar\gamma_{\mathcal{SD}}^2\bar\gamma_{\mathcal{SR}}}{\bar\gamma_{\mathcal{SD}}\bar\gamma_{\mathcal{SR}}+\bar\gamma_{\mathcal{SD}}\bar\gamma_{\mathcal{SE}}+\bar\gamma_{\mathcal{SR}}\bar\gamma_{\mathcal{SE}}}}{\bar\gamma_{\mathcal{RD}}-\bar\gamma_{\mathcal{SD}}}\\ =& \frac{\bar\gamma_{\mathcal{RD}}\bar\gamma_{\mathcal{SE}}(\bar\gamma_{\mathcal{SD}}\bar\gamma_{\mathcal{SR}}+\bar\gamma_{\mathcal{SD}}\bar\gamma_{\mathcal{SE}}+\bar\gamma_{\mathcal{SR}}\bar\gamma_{\mathcal{SE}})+\bar\gamma_{\mathcal{SR}}\bar\gamma_{\mathcal{SE}}^2(\bar\gamma_{\mathcal{SD}}+\bar\gamma_{\mathcal{SR}})}{(\bar\gamma_{\mathcal{RD}}\bar\gamma_{\mathcal{SR}}+\bar\gamma_{\mathcal{RD}}\bar\gamma_{\mathcal{SE}}+\bar\gamma_{\mathcal{SR}}\bar\gamma_{\mathcal{SE}})(\bar\gamma_{\mathcal{SD}}\bar\gamma_{\mathcal{SR}}+\bar\gamma_{\mathcal{SD}}\bar\gamma_{\mathcal{SE}}+\bar\gamma_{\mathcal{SR}}\bar\gamma_{\mathcal{SE}})}\\ \triangleq& P_0^{(RT)}.\end{aligned} \tag{58}$$

$$\begin{aligned}\Delta<0 &\Leftrightarrow \bar\gamma_{\mathcal{SR}}\bar\gamma_{\mathcal{SD}}^2\bar\gamma_{\mathcal{RD}}+\bar\gamma_{\mathcal{SR}}\bar\gamma_{\mathcal{SD}}^2\bar\gamma_{\mathcal{SE}}+\bar\gamma_{\mathcal{SD}}^2\bar\gamma_{\mathcal{RD}}\bar\gamma_{\mathcal{SE}}<\bar\gamma_{\mathcal{SR}}^2\bar\gamma_{\mathcal{SD}}\bar\gamma_{\mathcal{RD}}+\bar\gamma_{\mathcal{SR}}^2\bar\gamma_{\mathcal{RD}}\bar\gamma_{\mathcal{SE}}\\ &\Leftrightarrow \bar\gamma_{\mathcal{SR}}(\bar\gamma_{\mathcal{RD}}\bar\gamma_{\mathcal{SD}}^2-\bar\gamma_{\mathcal{RD}}\bar\gamma_{\mathcal{SR}}\bar\gamma_{\mathcal{SE}}+\bar\gamma_{\mathcal{SD}}^2\bar\gamma_{\mathcal{SE}})+\bar\gamma_{\mathcal{SD}}\bar\gamma_{\mathcal{RD}}(\bar\gamma_{\mathcal{SD}}\bar\gamma_{\mathcal{SE}}-\bar\gamma_{\mathcal{SR}}^2)<0\\ &\Leftrightarrow \bar\gamma_{\mathcal{SR}}[\bar\gamma_{\mathcal{RD}}(\bar\gamma_{\mathcal{SD}}^2-\bar\gamma_{\mathcal{SR}}\bar\gamma_{\mathcal{SE}}/2)+\bar\gamma_{\mathcal{SE}}(\bar\gamma_{\mathcal{SD}}^2-\bar\gamma_{\mathcal{SR}}\bar\gamma_{\mathcal{RD}}/2)]+\bar\gamma_{\mathcal{SD}}\bar\gamma_{\mathcal{RD}}(\bar\gamma_{\mathcal{SD}}\bar\gamma_{\mathcal{SE}}-\bar\gamma_{\mathcal{SR}}^2)<0.\end{aligned} \tag{59}$$

[7] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity - Part I. System description," *IEEE Trans. Commun.*, vol. 51, no. 11, pp. 1927–1938, Nov. 2003.

[8] G. Han, J. Jiang, C. Zhang, T. Q. Duong, M. Guizani and G. K. Karagiannidis, "A survey on mobile anchor node assisted localization in wireless sensor networks," *IEEE Commun. Surveys & Tut.*, vol. 18, no. 3, pp. 2220–2243, third quarter 2016.

[9] H. Q. Tran, C. V. Phan, and Q.-T. Vien, "An overview of 5G technologies." In: *Emerging Wireless Communication & Network Technologies: Principle, Paradigm and Performance*, Springer, pp 59–80, 2018.

[10] J. Laneman, D. Tse, and G. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[11] C. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[12] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[13] J. Vilela, M. Bloch, J. Barros, and S. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 256–266, Jun. 2011.

[14] I. Krikidis, J. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[15] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 682–694, Apr. 2013.

[16] E. Tekin and A. Yener, "The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[17] ——, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

[18] Y. Liu, A. P. Petropulu, and H. V. Poor, "Joint decode-and-forward and jamming for wireless physical layer security with destination assistance," in *Proc. ASILOMAR 2011*, Pacific Grove, CA, USA, Nov. 2011, pp. 109–113.

[19] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[20] R. Bassily and S. Ulukus, "Deaf cooperation and relay selection strategies for secure communication in multiple relay networks," *IEEE Trans. Signal Process.*, vol. 61, no. 6, pp. 1544–1554, Mar. 2013.

[21] R. Ahlswede, N. Cai, S.-Y. Li, and R. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[22] R. Koetter and M. Medard, "An algebraic approach to network coding," *IEEE/ACM Trans. Netw.*, vol. 11, no. 5, pp. 782–795, Oct. 2003.

[23] S. Zhang, S. C. Liew, and P. P. Lam, "Hot topic: Physical-layer network coding," in *Proc. ACM MobiCom'06*, Los Angeles, CA, USA, Sep. 2006, pp. 358–365.

[24] Q.-T. Vien, H. X. Nguyen, B. G. Stewart, J. Choi, and W. Tu, "On the energy-delay tradeoff and relay positioning of wireless butterfly networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 1, pp. 159–172, Jan. 2015.

[25] Q.-T. Vien, W. Tu, H. X. Nguyen, and R. Trestian, "Cross-layer topology design for network coding based wireless multicasting," *Computer Networks*, vol. 88, pp. 27-39, Sep. 2015

[26] Q.-T. Vien and H. X. Nguyen, "Network coding-based channel quality indicator reporting for two-way multi-relay networks," *Wireless Communications and Mobile Computing*, vol. 14, no. 15, pp. 1471–1483, Oct. 2014.

[27] Q.-T. Vien, B. G. Stewart, H. Tianfield, and H. X. Nguyen, "Cooperative retransmission for wireless regenerative multirelay networks," *IEEE Trans. Veh. Technol.*, vol. 62, no. 2, pp. 735–747, Feb. 2013.

[28] Q.-T. Vien, H. X. Nguyen, J. Choi, B. G. Stewart, and H. Tianfield, "Network coding-based block acknowledgement scheme for wireless regenerative relay networks," *IET Commun.*, vol. 6, no. 16, pp. 2593–2601, Nov. 2012.

[29] Q.-T. Vien, L.-N. Tran, and E.-K. Hong, "Network coding-based retransmission for relay aided multisource multicast networks," *EURASIP J Wireless Commun. Netw.*, vol. 2011, Article ID 643920, 10 pages, Dec. 2011.

[30] T. Cui, T. Ho, and J. Kliewer, "On secure network coding with nonuniform or restricted wiretap sets," *IEEE Trans. Inf. Theory*, vol. 59, no. 1, pp. 166–176, Jan. 2013.

[31] N. Cai and R. Yeung, "Secure network coding on a wiretap network," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 424–435, Jan. 2011.

[32] F. Gabry, R. Thobaben, and M. Skoglund, "Outage performances for amplify-and-forward, decode-and-forward and cooperative jamming strategies for the wiretap channel," in *Proc. IEEE WCNC'11*, Cancun, Mexico, Mar. 2011, pp. 1328–1333.

[33] R. Bassily and S. Ulukus, "Secure communication in multiple relay networks through decode-and-forward strategies," *J. Commun and Netw.*, vol. 14, no. 4, pp. 352–363, Aug. 2012.

[34] S. W. Kim, "Modify-and-forward for securing cooperative relay communications," in *International Zurich Seminar on Communications (IZS)*, Zurich, Switzerland, Feb. 2014, pp. 136–139.

[35] Q.-T. Vien, T. A. Le, H. X. Nguyen, and H. Phan, "A secure network coding based modify-and-forward scheme for cooperative wireless relay networks," in *Proc. IEEE VTC 2016-Spring*, Nanjing, China, May 2016, pp. 1–5.

[36] Q.-T. Vien, T. A. Le and T. Q. Duong, "Opportunistic secure transmission for wireless relay networks with modify-and-forward protocol," in *Proc. IEEE ICC 2017*, Paris, France, May 2017, pp. 1–6.

[37] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Design of an OFDM physical layer encryption scheme," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2114–2127, Mar. 2017.

[38] B. He, X. Zhou, and A. L. Swindlehurst, "On secrecy metrics for physical layer security over quasi-static fading channels," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6913–6924, Oct. 2016.

[39] M. Baldi, F. Chiaraluce, N. Laurenti, S. Tomasin, and F. Renna, "Secrecy transmission on parallel channels: Theoretical limits and performance of practical codes," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1765–1779, Nov. 2014.

[40] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE ISIT'06*, Seattle, WA, USA, Jul. 2006, pp. 356–360.

[41] S. Zhang, L. Fan, M. Peng, and H. V. Poor, "Near-optimal modulo-and-forward scheme for the untrusted relay channel", *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2545–2556, May 2016.

[42] G. Smith, "Quantifying information flow using min-entropy," in *Proc. QEST 2011*, Aachen, Germany, Sep. 2011, pp. 159–167.

[43] M. K. Simon and M.-S. Alouini, *Digital Communication over Fading Channels*, 2nd ed. John Wiley & Sons, 2005.

[44] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. Academic Press, 2007.

[45] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*, 4th ed. Mc-Graw Hill, 2002.